Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About the COAP Proxy Server

The COAP protocol is designed for use with constrained devices. COAP works in the same way on constrained devices as HTTP works on servers in accessing information.

The comparison of COAP and HTTP is shown below:

- In the case of a webserver: HTTP is the protocol; TCP is the transport; and HTML is the most common information format transported.
- In case of a constrained device: COAP is the protocol; UDP is the transport; and JSON/link-format/CBOR is the popular information format.

COAP provides a means to access and control device using a similar GET/POST metaphor and restful API as in HTTP.

Related Topics
Configuring the COAP Proxy, on page 4
Restrictions for the COAP Proxy Server

The following restrictions apply to COAP proxy server:

- Switch cannot advertise itself as CoAP client using ipv6 broadcast (CSCuw26467).
- Support for Observe Not Implemented.
- Blockwise requests are not supported. We handle block-wise responses and can generate block-wise responses.
- DTLS Support is for the following modes only RawPublicKey and Certificate Based.
- Switch does not act as DTLS client. DTLS for endpoints only.
- Endpoints are expected to handle and respond with CBOR payloads.
- Client side requests are expected to be in JSON.
- Switch cannot advertise itself to other Resource Directories as IPv6, due to an IPv6 broadcast issue.
- Configuration of Fast PoE, Perpetual PoE or 2-event classification has to be done before physically connecting any endpoint. Alternatively do a manual shut/no-shut of the ports drawing power.
- Power to the ports will be interrupted in case of MCU firmware upgrade and ports will be back up immediately after the upgrade.

Supported Hardware for the COAP Proxy Server

COAP Proxy Server is supported on the following Catalyst 3850 Switch Models:

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Cisco IOS Image</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-C3850-24T-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48T-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-24P-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48P-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48F-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-24U-S</td>
<td>IP Base</td>
<td>Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply</td>
</tr>
<tr>
<td>Switch Model</td>
<td>Cisco IOS Image</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WS-C3850-48U-S</td>
<td>IP Base</td>
<td>Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply</td>
</tr>
<tr>
<td>WS-C3850-12S-S</td>
<td>IP Base</td>
<td>Stackable 12 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-24S-S</td>
<td>IP Base</td>
<td>Stackable 24 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-12XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply</td>
</tr>
<tr>
<td>WS-C3850-16XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply. 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-S switch.</td>
</tr>
<tr>
<td>WS-C3850-24XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-32XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply. 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-S switch.</td>
</tr>
<tr>
<td>WS-C3850-48XS-S</td>
<td>IP Base</td>
<td>Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WSC3850-48XS-F-S</td>
<td>IP Base</td>
<td>Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24XU-S</td>
<td>IP Base</td>
<td>Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24T-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48T-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-24P-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48P-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48F-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Services feature set</td>
</tr>
</tbody>
</table>
### Switch Model | Cisco IOS Image | Description
--- | --- | ---
WS-3850-24U-E | IP Services | Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply
WS-3850-48U-E | IP Services | Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply
WS-C3850-12S-E | IP Services | Stackable, 2 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-24S-E | IP Services | Stackable, 24 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-12XS-E | IP Services | Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350-W power supply.
WS-C3850-16XS-E | IP Services | Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply.
16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-E switch.
WS-C3850-24XS-E | IP Services | Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.
WS-C3850-32XS-E | IP Services | Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.
32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-E switch.
WS-C3850-48XS-E | IP Services | Stackable, SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.
WS-C3850-48XS-E | IP Services | Stackable, SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.
WS-C3850-24XU-E | IP Services | Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100-W power supply.

### How to Configure the COAP Proxy Server

To configure the COAP proxy server, you can configure the COAP Proxy and COAP Endpoints in the Configuration mode.

The commands are: `coap [proxy | endpoints].`

### Configuring the COAP Proxy

To start or stop the COAP proxy on the switch, perform the steps given below:
## Configuring COAP Proxy

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | **enable** | Enables privileged EXEC mode.  
**Example:**  
Device> **enable** |
| Step 2 | **configure terminal** | Enters global configuration mode.  
**Example:** |
| Step 3 | **coap proxy** | Enters the COAP proxy sub mode.  
**Note** To stop the coap proxy and delete all configurations under coap proxy, use the **no coap proxy** command.  
**Example:**  
Device(config)# **coap proxy** |
| Step 4 | **security** *none* [ipv4 | ipv6] [ip-address ip-mask/prefix] | Takes the encryption type as argument. The two security modes supported are **none** and **dtls**  
*Note* To delete all security configurations under coap proxy, use the **no security** command.  
**Example:**  
Device(config-coap-proxy)# **security none** ipv4 1.1.0.0 255.255.0.0 |
| Step 5 | **max-endpoints** *number* | (Optional) Specifies the maximum number of endpoints that can be learnt on the switch. The default value is 10. The range is 1 to 500.  
**Note** To delete all max-endpoints configured under coap proxy, use the **no max-endpoints** command.  
**Example:**  
Device(config-coap-proxy)# **max-endpoints** 10 |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td><code>port-unsecure {port-num}</code></td>
<td>(Optional) Configures a port other than the default 5683. The range is 1 to 65000.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td><strong>Note</strong> To delete all port configurations under coap proxy, use the no <code>port-unsecure</code> command.</td>
</tr>
<tr>
<td></td>
<td>Device(config-coap-proxy)#<code>port-unsecure 5683</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>port-dtls {port-num}</code></td>
<td>(Optional) Configures a port other than the default 5684.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td><strong>Note</strong> To delete all dtls port configurations under coap proxy, use the no <code>port-dtls</code> command.</td>
</tr>
<tr>
<td></td>
<td>Device(config-coap-proxy)#<code>port-dtls 5864</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>`resource-directory [ipv4</td>
<td>ipv6] {ip-address}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td><strong>Note</strong> To delete all resource directory configurations under coap proxy, use the no <code>resource-directory</code> command.</td>
</tr>
<tr>
<td></td>
<td>Device(config-coap-proxy)#<code>resource-directory ipv4 192.168.1.1</code></td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>`list [ipv4</td>
<td>ipv6] {list-name}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td><strong>Note</strong> To delete any ip list on the COAP proxy server, use the no `list [ipv4</td>
</tr>
<tr>
<td></td>
<td>Device(config-coap-proxy)#<code>list ipv4 trial_list</code></td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td><code>start</code></td>
<td>Starts the COAP proxy on this switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-coap-proxy)#<code>start</code></td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td><code>stop</code></td>
<td>Stops the COAP proxy on this switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-coap-proxy)#<code>stop</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring COAP Endpoints

To configure the COAP Proxy to support multiple IPv4/IPv6 static-endpoints, perform the steps given below:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  * enable
    
    **Example:**
    Device> enable
  |
  Enables privileged EXEC mode.
  - Enter your password if prompted.

| **Step 2**
  * configure terminal
    
    **Example:**
    Device# configure terminal
  |
  Enters global configuration mode.

| **Step 3**
  * coap endpoint [ipv4 | ipv6] {ip-address}
    
    **Example:**
    Device(config)#coap endpoint ipv4 1.1.1.1
    Device(config)#coap endpoint ipv6 2001::1
  |
  Configures the static endpoints on the switch.
  - **ipv4** - Configures the IPv4 Static endpoints.
  - **ipv6** - Configures the IPv6 Static endpoints.
### Purpose

Command or Action | Purpose |
--- | --- |
To stop the coap proxy on any endpoint, use the **no coap endpoint** `[ipv4 | ipv6] {ip-address}` command. | **Note** |

**Step 4** exit

**Example:**

Device(config-coap-endpoint)# exit

**Step 5** end

**Example:**

Device(config)# end

### Monitoring COAP Proxy Server

To display the COAP protocol details, use the commands in the following table:

**Table 1: Commands to Display to COAP specific data**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show coap version</code></td>
<td>Shows the IOS COAP version and the RFC information.</td>
</tr>
<tr>
<td><code>show coap resources</code></td>
<td>Shows the resources of the switch and those learnt by it.</td>
</tr>
<tr>
<td><code>show coap endpoints</code></td>
<td>Shows the endpoints which are discovered and learnt.</td>
</tr>
<tr>
<td><code>show coap globals</code></td>
<td>Shows the timer values and end point values.</td>
</tr>
<tr>
<td><code>show coap stats</code></td>
<td>Shows the message counts for endpoints, requests and external queries.</td>
</tr>
<tr>
<td><code>show coap dtls-endpoints</code></td>
<td>Shows the dtls endpoint status.</td>
</tr>
</tbody>
</table>

**Table 2: Commands to Clear COAP Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear coap database</code></td>
<td>Clears the COAP learnt on the switch, and the internal database of endpoint information.</td>
</tr>
</tbody>
</table>

To debug the COAP protocol, use the commands in the following table:

**Table 3: Commands to Debug COAP protocol**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug coap database</code></td>
<td>Debugs the COAP database output.</td>
</tr>
</tbody>
</table>
### Examples: Configuring the COAP Proxy Server

This example shows how you can configure the port number 5683 to support a maximum of 10 endpoints.

```
Device# coap proxy security none ipv4 2.2.2.2 255.255.255.0 port 5683 max-endpoints 10
```

This example shows how to configure COAP proxy on `ipv4 1.1.0.0 255.255.0.0` with `no` security settings.

```
Device(config-coap-proxy)# security ?
  dtls  dtls
  none  no security

Device(config-coap-proxy)# security none ?
  ipv4  IP address range on which to learn lights
  ipv6  IPv6 address range on which to learn lights
  list  IP address range on which to learn lights

Device(config-coap-proxy)# security none ipv4 ?
  A.B.C.D {/nn || A.B.C.D} IP address range on which to learn lights

Device(config-coap-proxy)# security none ipv4 1.1.0.0 255.255.0.0
```

This example shows how to configure COAP proxy on `ipv4 1.1.0.0 255.255.0.0` with `dtls id trustpoint` security settings.

```
Device(config-coap-proxy)# security dtls ?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4  IP address range on which to learn lights
  ipv6  IPv6 address range on which to learn lights
  list  IP address range on which to learn lights

Device(config-coap-proxy)# security dtls id-trustpoint ?
  WORD  Identity TrustPoint Label

Device(config-coap-proxy)# security dtls id-trustpoint RSA-TRUSTPOINT ?
  verification-trustpoint Certificate Verification Label
```

---

**Note**

If you wish to disable the debugs, prepend the command with a "no" keyword.
Examples: Configuring the COAP Proxy Server

```
Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT

Device(config-coap-proxy)#security dtls ?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4 IP address range on which to learn lights
  ipv6 IPv6 address range on which to learn lights
  list IP address range on which to learn lights

Device(config-coap-proxy)#security dtls ipv4 1.1.0.0 255.255.0.0

Device(config-coap-proxy)#security dtls id-trustpoint?
  WORD Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT?
  WORD Identity TrustPoint Label
```

Note

For configuring `ipv4` / `ipv6` / `list`, the `id-trustpoint` and (optional) `verification-trustpoint`, should be pre-configured, else the system shows an error.

This example shows how to configure a Trustpoint. This is a pre-requisite for COAP `security dtls` with `id trustpoint` configurations.

```
ip domain-name myDomain
crypto key generate rsa general-keys exportable label MyLabel modulus 2048

Device(config)#crypto pki trustpoint MY_TRUSTPOINT
Device(ca-trustpoint)#rsakeypair MyLabel 2048
Device(ca-trustpoint)#enrollment selfsigned
Device(ca-trustpoint)#exit

Device(config)#crypto pki enroll MY_TRUSTPOINT
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
```

This example shows how to configure COAP proxy on `ipv4 1.1.0.0 255.255.0.0` with `dtls verification trustpoint` (DTLS with certificates or verification trustpoints)

```
Device(config-coap-proxy)#security dtls ?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4 IP address range on which to learn lights
  ipv6 IPv6 address range on which to learn lights
  list IP address range on which to learn lights

Device(config-coap-proxy)#security dtls id-trustpoint ?
  WORD Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT ?
  WORD Identity TrustPoint Label
  verification-trustpoint Certificate Verification Label <cr>

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT verification-trustpoint ?
  WORD Identity TrustPoint Label
```

Configuring COAP Proxy Server
CA-TRUSTPOINT
<cr>
------------------------------------------------------------------------------------------------
This example shows how to configure Verification Trustpoint. This is a pre-requisite for COAP security dtls with verification trustpoint configurations.

Device(config)#crypto pki import CA-TRUSTPOINT pkcs12 flash:hostA.p12 password cisco123
% Importing pkcs12...
Source filename [hostA.p12]?
Reading file from flash:hostA.p12
CRYPTO_PKI: Imported PKCS12 file successfully.

------------------------------------------------------------------------------------------------
This example shows how to create a list named trial-list, to be used in the security [ none | dtls ] command options.

Device(config-coap-proxy)#list ipv4 trial_list
Device (config-coap-proxy-iplist)#1.1.0.0 255.255.255.0
Device (config-coap-proxy-iplist)#2.2.0.0 255.255.255.0
Device (config-coap-proxy-iplist)#3.3.0.0 255.255.255.0
Device (config-coap-proxy-iplist)#exit
Device (config-coap-proxy)#security none list trial_list

------------------------------------------------------------------------------------------------
This example shows all the negation commands available in the coap-proxy sub mode.

Device(config-coap-proxy)#no ?
ip-list Configure IP-List
max-endpoints maximum number of endpoints supported
port-unsecure Specify a port number to use
port-dtls Specify a dtls-port number to use
resource-discovery Resource Discovery Server
security CoAP Security features

------------------------------------------------------------------------------------------------
This example shows how you can configure multiple IPv4/IPv6 static-endpoints on the coap proxy.

Device (config)# coap endpoint ipv4 1.1.1.1
Device (config)# coap endpoint ipv4 2.1.1.1
Device (config)# coap endpoint ipv6 2001::1

------------------------------------------------------------------------------------------------
This example shows how you can display the COAP protocol details.

Device#show coap version
CoAP version 1.0.0
RFC 7252

Device#show coap resources
Link format data -
</>
</1.1.1.6/cisco/context>
</1.1.1.6/cisco/actuator>
</1.1.1.6/cisco/sensor>
</1.1.1.6/cisco/lldp>
Device# show coap globals
Coap System Timer Values:
   - Discovery: 120 sec
   - Cache Exp: 5 sec
   - Keep Alive: 120 sec
   - Client DB: 60 sec
   - Query Queue: 500 ms
   - Ack delay: 500 ms
   - Timeout: 5 sec
Max Endpoints: 10
Resource Disc Mode: POST

Device# show coap stats
Coap Stats:
   - Endpoints: 2
   - Requests: 20
   - Ext Queries: 0

Device# show coap endpoints
List of all endpoints:

<table>
<thead>
<tr>
<th>#</th>
<th>Status</th>
<th>Age(s)</th>
<th>LastWKC(s)</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>D</td>
<td>10</td>
<td>94</td>
<td>1.1.1.6</td>
</tr>
<tr>
<td>2</td>
<td>D</td>
<td>6</td>
<td>34</td>
<td>1.1.1.5</td>
</tr>
</tbody>
</table>

Endpoints - Total: 2 Discovered: 2 New: 0

Device# show coap dtls-endpoints

<table>
<thead>
<tr>
<th>#</th>
<th>Index</th>
<th>State</th>
<th>String State</th>
<th>Value</th>
<th>Port</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>SSLOK</td>
<td>3</td>
<td>48969</td>
<td>20.1.1.30</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>SSLOK</td>
<td>3</td>
<td>53430</td>
<td>20.1.1.31</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>SSLOK</td>
<td>3</td>
<td>54133</td>
<td>20.1.1.32</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>SSLOK</td>
<td>3</td>
<td>48236</td>
<td>20.1.1.33</td>
<td></td>
</tr>
</tbody>
</table>

This example shows all options available to debug the COAP protocol.

Device# debug coap?
all: Debug CoAP all
database: Debug CoAP Database
errors: Debug CoAP errors
events: Debug CoAP events
packet: Debug CoAP packet
Related Topics

- Configuring the COAP Proxy, on page 4
- Information About the COAP Proxy Server, on page 1